Time for action!

Deliver **SECURELY** to anywhere with GitHub Actions!

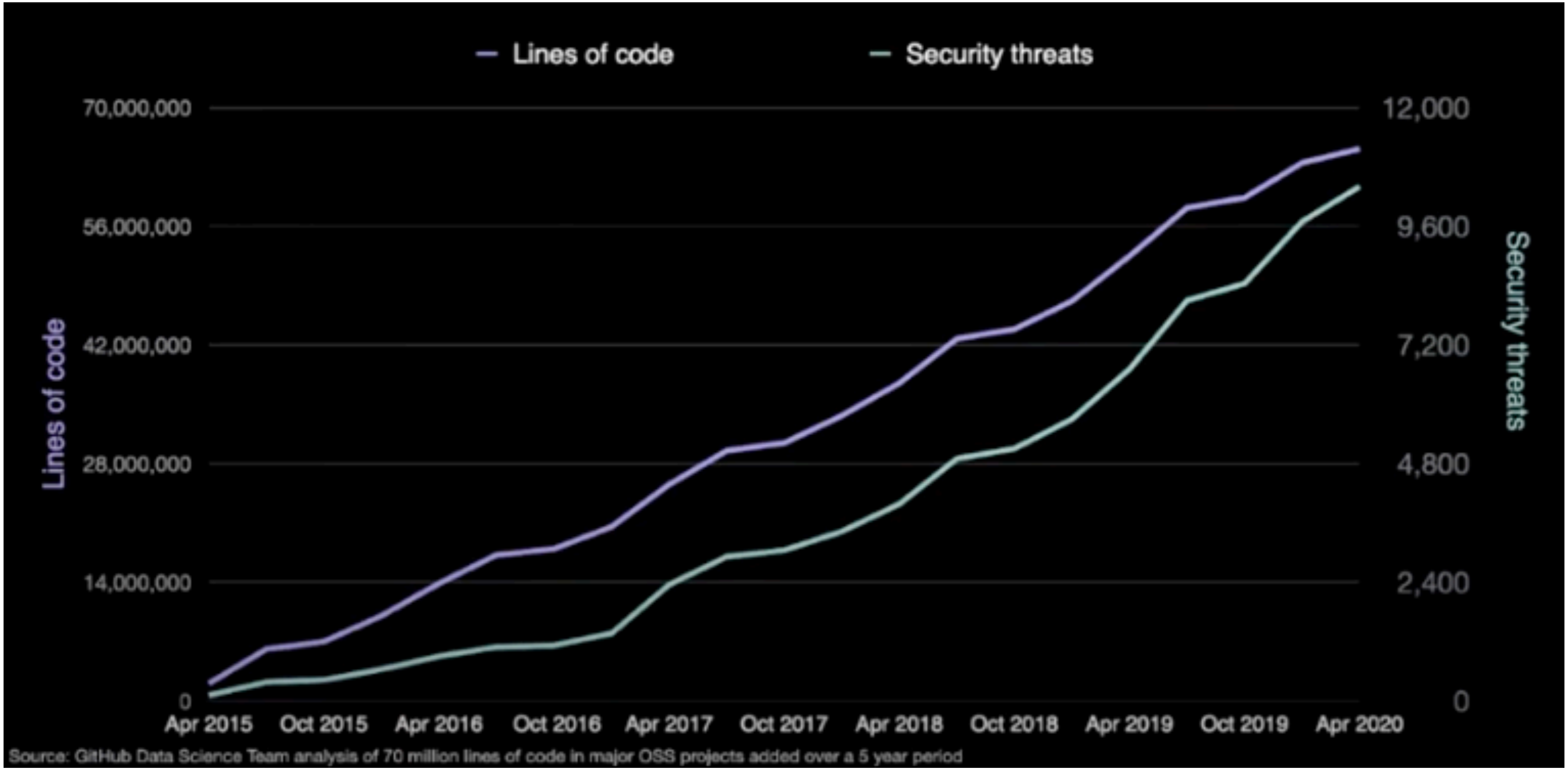
Victoria Almazova

@texnokot

What we will learn today

- DevSecOps: Devs and Security works together
- How GitHub is helping
- Adding on the top – 3rd party integrations
- Summary and action points

What’s the problem?



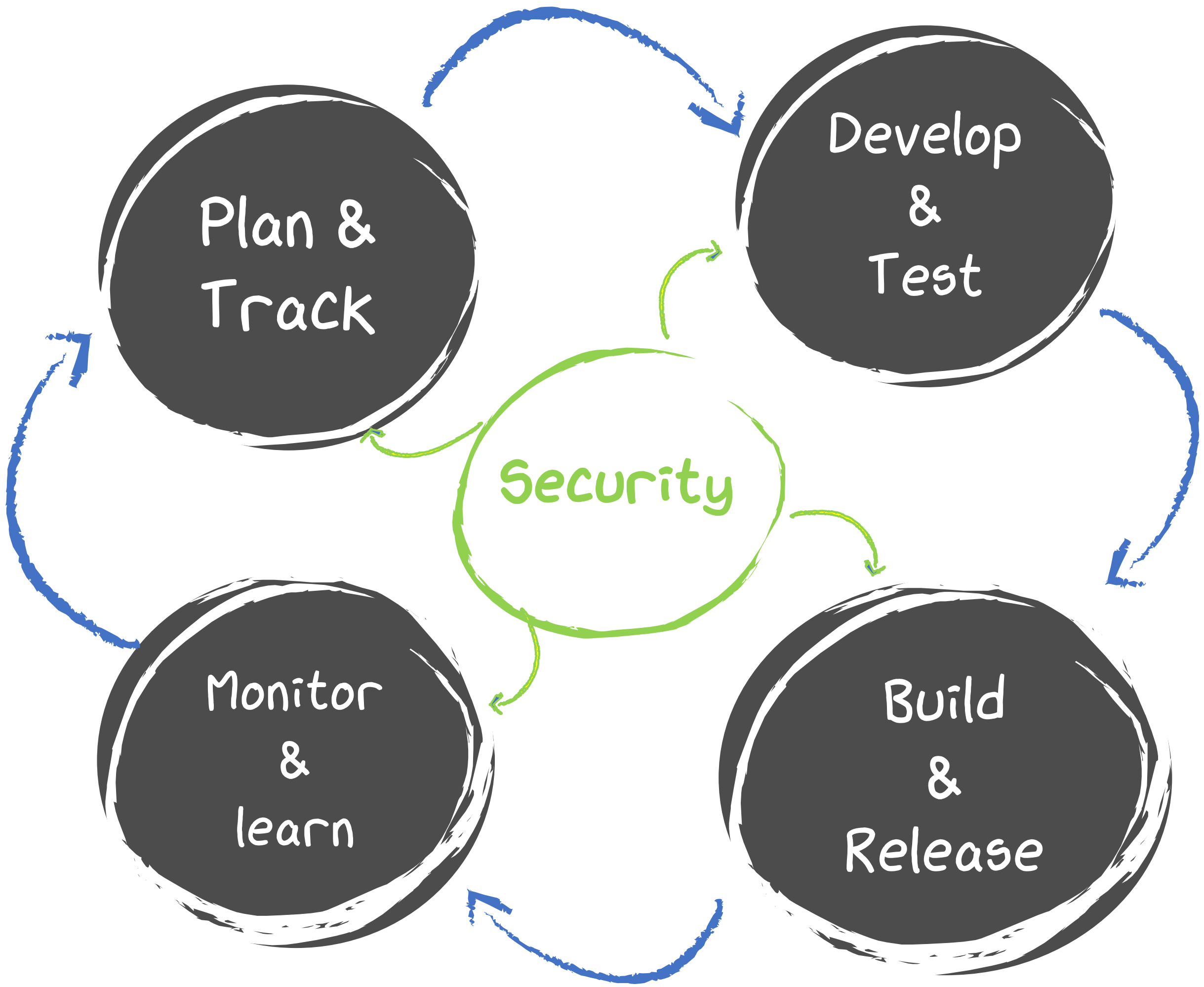
Source: GitHub Data Science Team analysis of 70 million lines of code in major OSS projects added over a 5 year period

DevSecOps

DevSecOps is the philosophy of integrating security practices within the DevOps process. ***#SecurityFirst*** culture!

DevSecOps is about introducing security earlier in the lifecycle of development, thus minimizing vulnerabilities and bringing security closer to IT and business objectives

@JFrog



DevSecOps at the glance

Pre-commit

- ✗ Threat modeling
- ✗ IDE Security plugins
- ✗ Pre-commit hooks
- ✗ Secure coding standards
- ✗ Peer review

Commit (CI)

- ✗ Static code analysis
- ✗ Security unit tests
- ✗ Dependency management

Acceptance (CD)

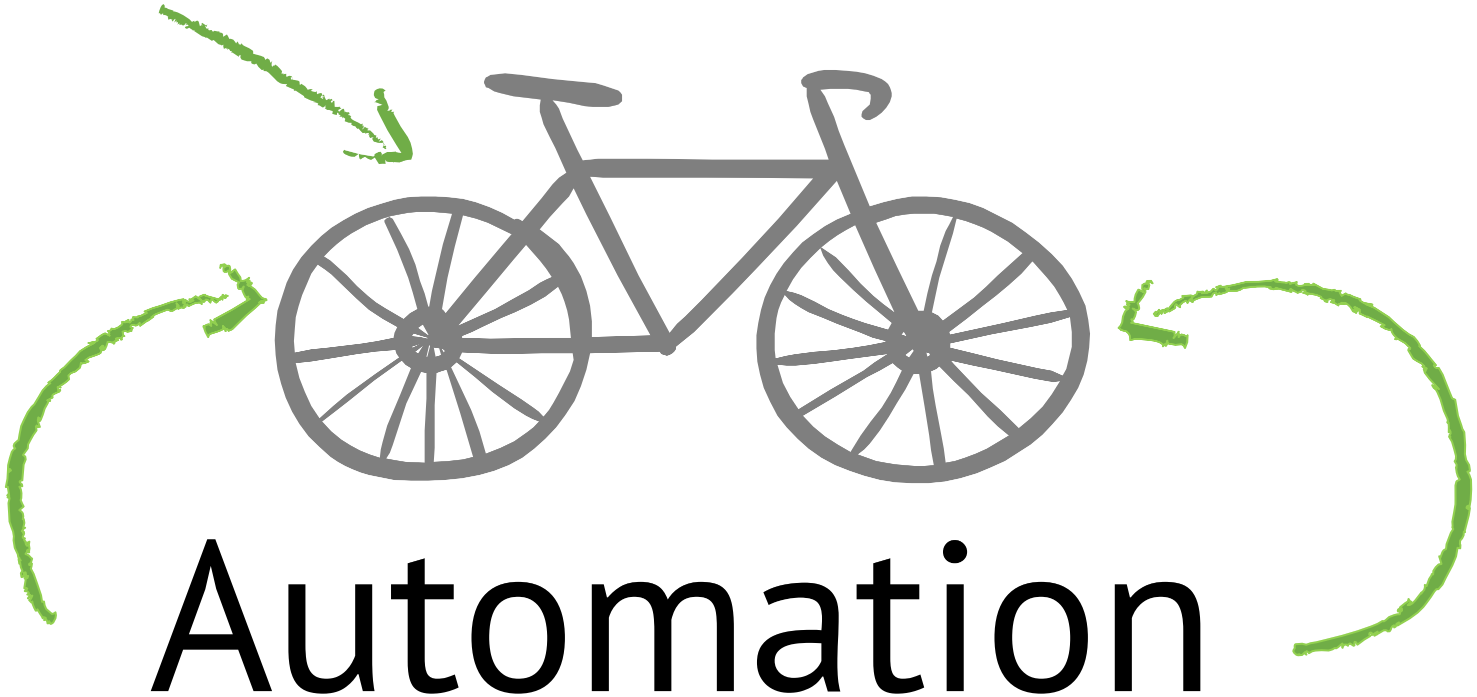
- ✗ Infrastructure as Code
- ✗ Security scanning
- ✗ Cloud configuration
- ✗ Security acceptance testing

Production

- ✗ Security smoke tests
- ✗ Configuration checks
- ✗ Penetration testing

Operations

- ✗ Continuous monitoring
- ✗ Threat intelligence
- ✗ Penetration testing
- ✗ Blameless postmortems



Automation

Why not to automate security then?

How GitHub is helping

- GitHub Advanced Security
- CodeQL
- Dependabot
- Security policies and branch protections
- Audit logging and documented changes via PRs

Show me

Adding on the top – 3rd party integrations

- Static analysis tools
- Infrastructure as code
- Container security

Show me

What we learned today

- DevSecOps: it is a lot about automation in CI/CD
- Dependabot and CodeQL can cover 80% of your security needs
- SARIF openned the door for the 3rd party integrations

Summary and action points

- Easy start with Dependabot
- CodeQL is a powerful tool, but requires resources…
- Tools are tools, but human resources and prioritization are important
- ToDo:
    - Explore what is available out the box and start small: Dependabot
    - Branch protection must have
    - Don’t overload CodeQL be rational -> increases check time and frustrates developers

Resources

- GitHub about DevSecOps: https://github.blog/2020-08-13-secure-at-every-step-a-guide-to-devsecops-shifting-left-and-gitops/
- Finding security vulnerabilities in JavaScript with CodeQL - GitHub Satellite 2020: https://www.youtube.com/watch?v=pYzfGaLTqC0&ab_channel=GitHub
- CodeQL documentation: https://help.semmle.com/codeql/index.html
- CodeQL libraries and queries: https://github.com/github/codeql
- 3rd party integration:
  - https://github.blog/2020-10-05-announcing-third-party-code-scanning-tools-static-analysis-and-developer-security-training/
  - https://github.blog/2020-10-07-announcing-third-party-code-scanning-tools-infrastructure-as-code-and-container-scanning/
- GitHub roadmap: https://github.com/github/roadmap/projects/1

Thanks!

Any questions?

You can find me at
@texnokot
victoria.almazova@microsoft.com